

MEDIAPRO[®]

Learn. Improve. Succeed.

The Challenge of Creating an Adaptive Awareness Program

Tom Pendergast, Ph.D.
Chief Strategist
MediaPro



Outline

The Tier 4 Challenge

The Adaptive Awareness Framework

Putting the Framework into Action



The Tier 4 Challenge

Predictive Indicators

Continuous Improvement

Adapts and Responds

Part of the Culture

predictive indicators

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity risk management process based on lessons learned and predictive indicators derived from previous activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- *Integrated Cybersecurity Risk Management* – An organization-wide approach to managing cybersecurity risk through policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- *External Participation* – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

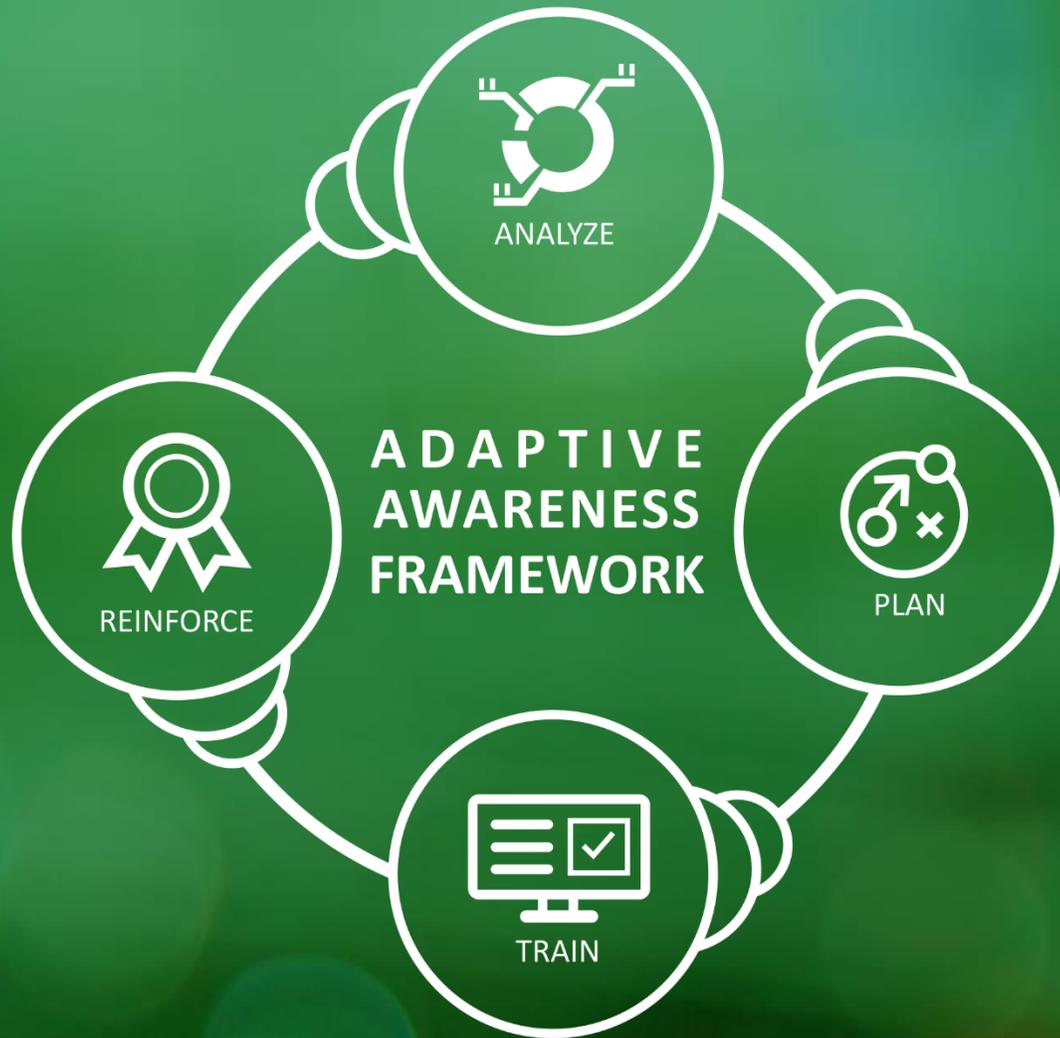
continuous improvement

actively adapts

part of organizational culture

2.3 Framework

The Framework Profile (Profile) is the alignment of the Functions, Categories, and



Adaptive Awareness

Analyze

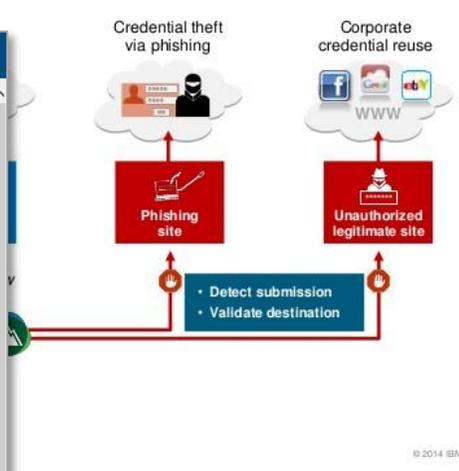
Plan

Train

Reinforce

Analyze

IBM Security Systems IBM
Trusteer Apex - Corporate Credentials Protection



PHISHME

Products & Services | The PhishMe Advantage | Resources | News & Events | Company

Blog | Contact | Request a Demo

PRODUCT & SERVICES / PHISHME REPORTER

PhishMe Reporter

Real detection and intelligence is critical for security operations and incident response teams to minimize the time an attacker is on a network or "detection deficit". To date, organizations have lacked an efficient process for identifying, organizing, and analyzing user reports of suspicious emails that may indicate early stages of a cyber attack. PhishMe Reporter™ provides organizations with a simple, cost-effective way to fill this information gap.

PhishMe Reporter is a patented technology in the PhishMe solution, improves an organization's threat detection capabilities by analyzing and normalizing user reports of phishing attempts, as a result, transforming users into a proactive line of human security sensors.

Resources

- Infographics
- Videos
- Webinars
- Whitepapers

observe it INSIDER THREAT INTELLIGENCE | MANAGEMENT CONSOLE

Welcome, Observerrit.Authentication Admin | Sign out

Time period: 1/24/16 12:00 AM - 2/23/16 6:10 PM

USER RISK DASHBOARD

USER RISK SUMMARY

14 RISKY USERS

4 NEW USERS AT RISK

TOP RISK APPLICATIONS

- 8 | Windows Explorer
- 6 | SSH, Telnet and Rlogin client
- 7 | Microsoft Management Console
- 3 | Notepad++ - a free (GNU) so...
- 3 | SQL Server Management Studio

TOP RISK ALERTS

- 7 | USB or similar device inserted...
- 6 | user started Putty Session
- 1 | Backdoor detected - Execut...
- 1 | Edit application file in C:\Pro...
- 1 | Privilege elevation - Prevent...

RISKY USERS (14)

User name: Daniel Petri (Support) | Score: 49 | 16

RISKY APPLICATIONS

- 45% Windows Explorer
- 18% SQL Server Management Studio
- 9% Windows Command Processor

ALERTS

- 8 | USB or similar device inserted - autoplay started, 1 | Unauthorized USB drive Accessed
- 2 | SQL Server Management Studio, 1 | sql, 1 | properties
- 2 | user started CMD.exe (Windows Command Processor)

MEDIAPRO Dashboard

DASHBOARD

Performance Metrics

Security IQ

"Security IQ" is a blended score based on knowledge assessment score, phishing performance, and training completions.

93

Q4 2015

Key Stats

Program Term: 1/1/15 to 12/31/16

- Total trained: 15,416 (94%)
- Total phished: 15,088 (92%)
- Total surveyed: 7,544 (46%)

Training Vs Phishing Overview

© 2016 MEDIAPRO HOLDINGS, LLC ALL RIGHTS RESERVED

Captcha Form: 204

Feedback Form: 3

Form Submitted: 3

File Downloaded: 5

File Upload: 10

Password Submitted: 170

Page: 2,090

Unsubscribe Page: 1

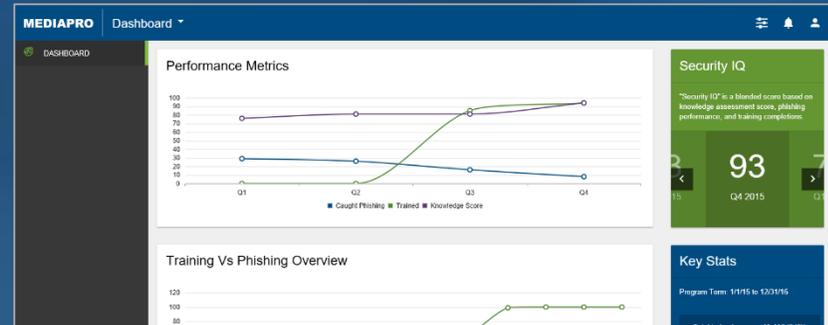
of Hits: 1,531

Each web activity, or "hit", represents one access to a web page resource by a browser or email client.

Action Page View: Shows the ratio of hits that were caused by the user

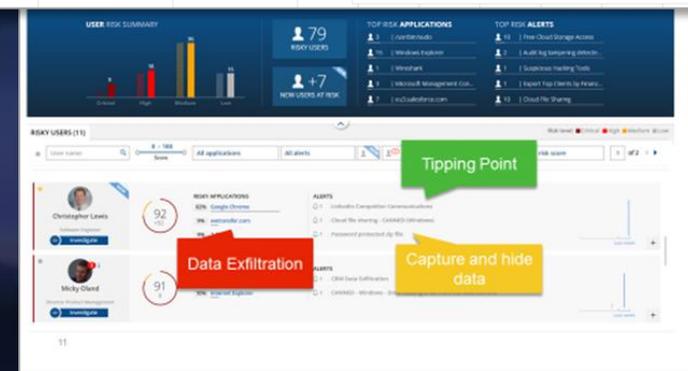
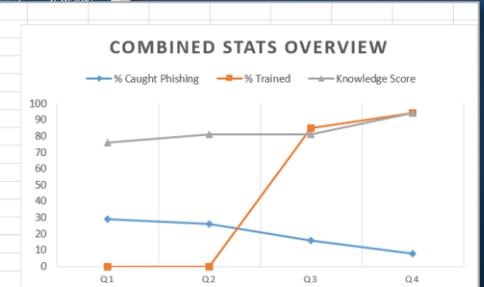
Analyze Options

- Surveys
- Phishing / Social Engineering
- Behavioral Analytics
- Incident Reporting
- Completion Rates
- Other?



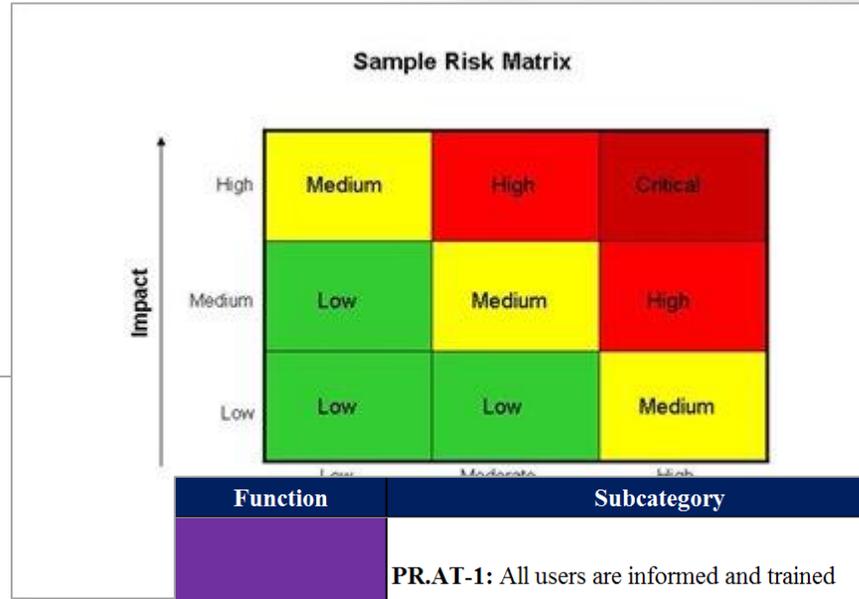
Combined Score Over Time				
	% Caught Phishing	% Trained	Knowledge Score	Security IQ
Q1	29	0	76	74
Q2	26	0	81	78
Q3	16	85	81	83
Q4	8	94	94	93

Training Vs Phishing Overview			
	% Caught Phishing	% Trained Security Basic	% of Overall Population Trained in Phishing
January	29	0	0
February	32	0	0
March	26	0	0
April	28	0	18
May	24	0	22
June	25	0	28
July	23	35	30
August	14	62	30
September	12	99	32
October	6	100	32
November	8	100	32
December	6	100	32



Plan

MEDIAPRO
Learn. Improve. Succeed.



Security Awareness Planning Toolkit

Function	Subcategory	Current State	Target State
	PR.AT-1: All users are informed and trained		
	PR.AT-2: Privileged users understand roles & responsibilities		
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities		

Security Awareness Roadmap

and transfer information. However, very little has been done to secure this "human" operating system, or HumanOS. As a result, people rather than machines are the primary security risk. Security awareness training is one of the most effective ways to address this problem. This roadmap is designed to help you understand, plan, and implement a security awareness program that reduces risk by changing behavior, increasing compliance, and audit requirements. To use this roadmap, first identify the current state of your program and where you want to go.

1 Compliance Focused

Program is designed primarily to meet compliance or audit requirements. Training is limited to annual or ad-hoc basis, and is not consistent across all employees, contractors, or third parties. Training is not tailored to the organization's specific risks, and how to identify, prevent, or report a security incident.

2 Promotes Awareness & Change

Program identifies the training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. Program goes beyond just annual training and includes continuous reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees, contractors and staff understand and follow organizational policies and actively recognize, prevent and report incidents.

3 Long-Term Sustainment

Program has processes and resources in place for a long-term cycle, including at a minimum an annual review and update of both training content and communication methods. As a result, the program is an established part of the organization's culture and is current and engaging.

4 How To Get There:

- Identify when you will review your awareness program each year.
- Identify new or changing technologies, trends, business requirements, or compliance standards that should be included in your annual update.
- Conduct an assessment of your organization's security awareness program and compare that to the benchmarks in step 2.
- Survey staff for feedback, including what elements they find most interesting, and what behaviors they identify.
- Review all the topics you are communicating and identify if new topics need to be added and which existing topics should be removed or updated.
- Once topics changes have been identified, review and update the training objectives for each topic.
- Review how the topics are communicated, which methods have had the greatest impact, and which need to be updated or dropped.
- Conduct an annual review and update of the budget to address changing business requirements.

5 Metrics Framework

Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. In addition, some set of metrics will be used in previous stages.

How To Get There:

- Identify key metrics that align to business outcomes.
- Document how and when you intend to measure the metrics.
- Identify who to communicate results to, when, and how.
- Execute metrics measurement.

Deliverables:

- Metrics matrix.

Examples of Metrics:

- Nbr. of people who take courses to monthly program assessments.
- Nbr. of monthly incident reports.
- Nbr. of people who completed the awareness training.
- Nbr. of users who passed the assessment.
- Employee scores from behavior testing.
- % of users aligned with positive attitude towards information security.
- % of users reported who believe their actions can have an impact on security.

Additional Materials:

- 1411 Strategies
- Building an Information Technology Security Awareness and Training Program
- ENISA Awareness Guide (2010)
- How to Raise Information Security Awareness
- 20 Critical Controls
- Twenty Critical Security Controls for Effective Cyber Defense

Documents followed by this icon may be downloaded at: www.securingthehuman.org/resources/planning

Security Awareness Risk and Intervention Matrix

IDENTIFY RISK	TARGET BEHAVIOR	TRAIN	REINFORCE	MEASURE
Employees are not identifying social engineering or phishing attempts and are thus allowing malware into the org	We want employees to rapidly recognize social engineering or phishing attempts of all kinds, and respond to those attempts following company policies.	<ul style="list-style-type: none"> Phishing topics in Security Basics course Phishing mini course Phishing full course 	<ul style="list-style-type: none"> Another Phishy E-mail animation Phishing posters CISO follow-up for frequent fails 	<ul style="list-style-type: none"> Survey for general ability to understand nature of problem Phish for e-mail violations Phone phish for phone social engineering USB drops
Employees are using company passwords at unapproved sites (against policy)	We want employees to only use company passwords on approved sites	<ul style="list-style-type: none"> Password topics in Security Basics 	<ul style="list-style-type: none"> Onscreen reporting from tool Password posters Manager follow-up 	<ul style="list-style-type: none"> Survey for understanding of policy Using password reporting to identify violations

Planning Options

- Identify Risks
- Target Behaviors
- Identify Tools (Training and Reinforcement)
- Plan to Measure
- Plan to Change

SANS: Securing the Human - Security Awareness Program Execution Checklist



Tasking	Completion	Comments
Plan Approved - Execute		Once plan is approved and signed off, you can execute your plan.
Source Training Materials		Develop or purchase materials for both primary and reinforcement training. If developing internally, identify complexity of materials and resources you require to develop them. If purchasing, be sure to review and test multiple vendors, ensuring content is high-quality, actively updated and meets your requirements.
Test Computer Based Training / Video Training		If your primary training is Computer Based Training (videos), identify where it will be hosted. If hosted internally, make sure training will load in your LMS. Once training is loaded in your LMS or vendor's LMS test all functionality, including login, bookmarking, quizzes and reporting. Technical issues with LMS are one of the most common challenges with most security awareness programs. Then load five to ten users into LMS, have LMS notify test users about training and have them take training. Be sure to test all browser types used in your organization.
Management Briefing		Brief management before rollout begins. Explain what security awareness is, the value to your organization and your overall plan. Include examples of the training. You may also want to train senior leadership at this time, in person.
Help Desk		Ensure help desk is briefed and understands your rollout plan. Give them an FAQ checklist so they can respond to end user questions/problems. If doing a phased rollout, you may want to make them one of the first groups you train.
Executive Announcement		Have a senior executive announce upcoming awareness training/program. Examples include organization-wide email, video or perhaps blog.
		If primary training is onsite instruction, send out email announcement and then provide onsite training. If primary training is CBT, load users into LMS and have LMS send out login notifications. Be sure to set a

Train

wombat security technologies

Safer Web Browsing
Lesson 3 - Browsing Best Practices

Browsing Adventure 0/2 Risky Decisions

Wombank

Go to www.wombank.com and log into your bank account.
login: jms1234
password: sPp9kkl1

Wombank

Bank Portfolio Invest Protect

Login

1 2 3

© 2011-2012 Wombat Security Technologies, Inc. All rights reserved.

Your Logo here

S-141: Security Awareness Fundamentals
Understanding Information Security Threats
What is Information Security?

Preventing Phishing
Refusing the Bait

MEDIAPRO

Catch the Phish!

Order Information

Manager Alexander Christensen (client@stockton.us)
To: Bill Smith

FedEx.

Tracking ID: 6921-84778120
Date: Monday, 25 February 2013, 10:22 AM

Dear Client,
Your parcel has arrived at February 27. Courier was unable to deliver the parcel to you at 27 February 06:33 PM.

To receive your parcel, please, print this receipt and go to the nearest office.

Print Receipt

Best Regards, The FedEx Team.

Reminders: You're Bill Smith of the Acme Company, bill.smith@acme.com. Drag each message to keep or delete.

KEEP

Screen 3 of 4

RESOURCES

inspired eLearning

v 4.7.12

Training Options

- Online or In-Person
- Build vs Buy
- Easy to Refresh/Customize
- Required or Not?
- Behavioral?



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



» How to use this course

Security Basics

- ✓ Understanding Threats
- ✓ Physical Security
- Safe Computing
- Assessment

COPYRIGHT © 2016 MEDIAPRO

last
page
visited

SANS Security Awareness Network

About | Products | Pricing | Resources | Events | Blog | Support | [Free Demo](#)

Resources: Security Awareness Posters

Posters can be a great way to communicate your message, such as the best way for ordinary computer users to protect themselves or a roadmap to help you plan, build and implement your security awareness program. These resources are developed by the community for the community. These posters are distributed under the [Creative Commons BY-NC-ND 3.0](#) license. You are welcome and encouraged to download, print and share these posters as long as you do not modify them. Please send any questions or any feedback on how to improve these resources to community@securingthehuman.org.

Creating a Cyber Secure Home

This poster walks families through the five key steps on how to create a cyber secure home. What makes this poster so powerful, is these are also the very same secure behaviors that most organizations want employees to exhibit at work.

- English Version
- Norwegian Version
- Hungarian Version
- Czech Version
- Turkish Version
- Russian Version

Protecting Healthcare Data

This poster explains to healthcare professionals what healthcare data is, why it needs to be protected, where it is located, and top tips on how to secure it. If your organization handles PHI this is a great resource to assist in your security awareness program.

- English Version
- European Spanish Version

MediaPro
Learn. Improve. Succeed.

MediaPro Reinforcement Videos

Protecting your data is too important to leave to once-a-year training. That's why we've created a series of videos to remind people about some key topics in data protection, like privacy, malware, phishing, and more.

Lucky Jane, Protecting Data on the Road

Jane's going off to a conference, and she's doing her part to protect company information when traveling for work.

FREE USB DRIVE
SCAN YOUR BADGE
DATA LOCK
P

EMAIL
TELEPHONE NUMBER
YOUR NAME
LOOK UP CHILDREN'S
FINGER PRINTS
ADDRESS
NATIONAL ID NUMBER
DATE OF BIRTH

12 Videos
2 Followers
1 Moderator

Reinforcement Options

- Cost
- Cultural Fit
- Logistics

ENISA European Union Agency for Network and Information Security

ABOUT | CAREERS | PUBLIC PROCUREMENT | SITE MAP | CONTACT

ENGLISH | BULGARIAN | ROMANIAN | GREEK

CEP | CIP & Resilience | Identity & Trust | Risk Management

Video clips

View or download our video clips and use them in any information security training programme, awareness activity and company website. Our video clips are great tools for raising information security awareness. ENISA has produced video clips which will make your employees aware of information security risks and remind them of appropriate good practices. The ENISA video clips are available for download and use in any information security training programme, awareness activity and company website.

To view a clip, please click on the clip. To download a clip in PPT-format, please click on the relevant flag. All clips are available in all 23 official EU languages.

Learn your computer (1) | Learn your password (2) | Protect your data.

Remember surfing (1) | Remember surfing (2) | Remember surfing (3)

SAC the security awareness COMPANY

Home | About | Contact | Freebies | Contact Us

Security Cat

Do you may be man's best friend, but Security Cat's got your back!

Posters

TREAT YOUR PASSWORDS LIKE YOUR UNDERWEAR
Check for freshness! | Stop from getting too close!

SECURITY CAT IS FLEXIBLE...
...BUT HIPAA RULES ARE NOT!

YOU'VE NEVER BACKED UP YOUR FILES!
...YOU GOTTA BE KITTEN ME!

YOU CLICKED ON THAT PHISHING LINK? THIS DISPLEASES SECURITY CAT
DON'T PANIC REPORT IT!

SECURITY CAT KNOWS HOW TO DISPOSE OF HARD DRIVES

SECURITY CAT IS ON YOUR COMPUTER, INSTALLING YOUR SOFTWARE UPDATES

Putting It All Together

Start with data: survey, phish, etc.

Draft a plan with flexibility in mind

Announce the program (and keep it positive)

Train

Reinforce continuously

Analyze and Adapt

- Keep gathering data
- Reinforce when identifying problems (phishing, UBA)
- Make it relevant (role-based)
- Use personal follow-up messages to reinforce pressure points

Thank You!

Tom Pendergast
tomp@mediapro.com
425-483-4734



